Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	1674	network near session	US-PGPUB; USPAT; EPO; DERWENT	OR	ON	2004/12/23 16:17
S2	3286	network near event	US-PGPUB; USPAT; EPO; DERWENT	OR	ON	2004/12/23 16:17
S3	1771	event near parameter	US-PGPUB; USPAT; EPO; DERWENT	OR	ON	2004/12/23 16:17
S4	47028	((network near message) or (message)) near transmit$3	US-PGPUB; USPAT; EPO; DERWENT	OR	ON	2004/12/23 16:17
S5	1489	network near stream	US-PGPUB; USPAT; EPO; DERWENT	OR	ON	2004/12/23 16:17
S6	92665	(NAT) or (Network near address near translation)	US-PGPUB; USPAT; EPO; DERWENT	OR	ON	2004/12/23 16:20
S7	5275	network near security	US-PGPUB; USPAT; EPO; DERWENT	OR	ON	2004/12/23 16:20
S8	343	S6 and S7	US-PGPUB; USPAT; EPO; DERWENT	OR	ON	2004/12/23 16:21
S9	145	S8 and session and event and parameter	US-PGPUB; USPAT; EPO; DERWENT	OR	ON	2004/12/23 16:27
S10	731	S6 and session and event and parameter	US-PGPUB; USPAT; EPO; DERWENT	OR	ON	2004/12/23 16:27
S11	396	S6 and session and event and parameter and stream	US-PGPUB; USPAT; EPO; DERWENT	OR	ON	2004/12/23 16:27
S12	122	S6 and S1	US-PGPUB; USPAT; EPO; DERWENT	OR	ON	2004/12/23 16:28
S13	1037	(709/200).ccls.	US-PGPUB; USPAT; EPO; DERWENT	OR	ON	2004/12/23 16:28

S14	10	S6 and S13	US-PGPUB; USPAT; EPO; DERWENT	OR	ON	2004/12/23 16:29
S15	7	S14 and session	US-PGPUB; USPAT; EPO; DERWENT	OR	ON	2004/12/23 16:29
S16	3	S15 and event	US-PGPUB; USPAT; EPO; DERWENT	OR	ON	2004/12/23 16:30
S17	3	S16 and parameter	US-PGPUB; USPAT; EPO; DERWENT	OR	ON	2004/12/23 16:30
S18	2	S17 and stream	US-PGPUB; USPAT; EPO; DERWENT	OR	ON	2004/12/23 16:30
S19	709	event near (aggregation or correlation)	US-PGPUB; USPAT	OR	ON	2004/12/28 14:49
S20	33224	NAT or (Network adj address adj translation)	US-PGPUB; USPAT	OR	ON	2004/12/28 14:49
S21	2326	intrusion adj detection	US-PGPUB; USPAT	OR	ON	2004/12/28 14:49
S22	1761	event near group$3	US-PGPUB; USPAT	OR	ON	2004/12/28 14:50
S23	12	(S19 or S22) and S20 and S21	US-PGPUB; USPAT	OR	ON	2004/12/28 14:52
S25	38	S20 near rule	US-PGPUB; USPAT	OR	ON	2004/12/28 14:54
S26	20474	event near (detect$ or monitor$)	US-PGPUB; USPAT	OR	ON	2004/12/28 14:54
S27	1	S25 and S26	US-PGPUB; USPAT	OR	ON	2004/12/28 14:56
S28	1	S25 and S21 and S19	US-PGPUB; USPAT	OR	ON	2004/12/28 14:56
S29	3	S25 and S21 and event	US-PGPUB; USPAT	OR	ON	2004/12/28 14:57
S30	3300	event near manag$5	US-PGPUB; USPAT	OR	ON	2004/12/28 14:58
S31	15	S30 near security	US-PGPUB; USPAT	OR	ON	2004/12/28 14:59
S32	236290	S21 or IDS	US-PGPUB; USPAT	OR	ON	2004/12/28 15:00
S33	19377	S32 and S20	US-PGPUB; USPAT	OR	ON	2004/12/28 15:00
S35	65	S33 and (S19 or S22)	US-PGPUB; USPAT	OR	ON	2004/12/28 15:09
S36	1466	network near session	US-PGPUB; USPAT	OR	ON	2004/12/28 15:09

S37	968	(S36 or session) and (event or S19) and S20	US-PGPUB; USPAT	OR	ON	2004/12/28 15:10
S38	73	(S36) and (event or S19) and S20	US-PGPUB; USPAT	OR	ON	2004/12/28 15:20
S39	3	S38 and S19	US-PGPUB; USPAT	OR	ON	2004/12/28 15:20
S40	1	("6122665").pn.	US-PGPUB; USPAT	OR	ON	2004/12/28 15:21
S41	0	S40 and S20	US-PGPUB; USPAT	OR	ON	2004/12/28 15:21
S42	1	("5717879").pn.	US-PGPUB; USPAT	OR	ON	2004/12/28 15:21
S43	0	S42 and S20	US-PGPUB; USPAT	OR	ON	2004/12/28 15:21
S44	1998	(709/224).CCLS.	USPAT; USOCR	OR	OFF	2004/12/28 15:35
S45	1474	(713/201).CCLS.	USPAT; USOCR	OR	OFF	2004/12/28 15:35
S46	267	(719/318).CCLS.	USPAT; USOCR	OR	OFF	2004/12/28 15:35
S47	780	(709/228).CCLS.	USPAT; USOCR	OR	OFF	2004/12/28 15:35
S48	753	(709/202).CCLS.	USPAT; USOCR	OR	OFF	2004/12/28 15:35
S51	103	S44 and S48	US-PGPUB; USPAT; EPO; DERWENT	OR	ON	2004/12/28 15:37
S53	88	S44 and S45	US-PGPUB; USPAT; EPO; DERWENT	OR	ON	2004/12/28 15:38
S54	3	S51 and S53	US-PGPUB; USPAT; EPO; DERWENT	OR	ON	2004/12/28 15:39
S55	24	S48 and S45	US-PGPUB; USPAT; EPO; DERWENT	OR	ON	2004/12/28 15:41
S56	9	S44 and S47 and S48	US-PGPUB; USPAT; EPO; DERWENT	OR	ON	2004/12/28 15:43
S57	0	"709.clas" and S45	US-PGPUB; USPAT; EPO; DERWENT	OR	ON	2004/12/28 15:43
S58	16940	("709").CLAS.	USPAT; USOCR	OR	OFF	2004/12/28 15:43
S59	597	S58 and S45	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2004/12/28 15:44

S60	1	S59 and S20 and S26	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2004/12/28 15:47
S61	28	S59 and S20	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2004/12/28 15:48
S62	30	S59 and (S20 or S19)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2004/12/28 15:48
S63	0	S61 not S62	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2004/12/28 15:48
S64	2	S62 not S20	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2004/12/28 15:48
S65	174364	packet	US-PGPUB; USPAT; EPO; DERWENT	OR	ON	2004/12/29 10:35
S66	5340557	group3 or associat$5 or correlat4 or relat$4	US-PGPUB; USPAT; EPO; DERWENT	OR	ON	2004/12/29 11:11
S68	1982671	transmission or stream or message or session	US-PGPUB; USPAT; EPO; DERWENT	OR	ON	2004/12/29 10:36
S69	9451	S65 near S66	US-PGPUB; USPAT	OR	ON	2004/12/29 10:37
S70	22846	S65 near S68	US-PGPUB; USPAT	OR	ON	2004/12/29 10:37
S71	92744	(NAT) or (Network near address near translation)	US-PGPUB; USPAT; EPO; DERWENT	OR	ON	2004/12/29 10:38
S72	5181	S69 and S70	US-PGPUB; USPAT; EPO; DERWENT	OR	ON	2004/12/29 10:38
S73	6	(S69 or S70) near S71	US-PGPUB; USPAT; EPO; DERWENT	OR	ON	2004/12/29 10:38
S74	121	(S69 or S70) same S71	US-PGPUB; USPAT; EPO; DERWENT	OR	ON	2004/12/29 14:28
S75	1742	synchroniz$6 near S65	US-PGPUB; USPAT; EPO; DERWENT	OR	ON	2004/12/29 11:12

S76	832	S75 same S68	US-PGPUB; USPAT; EPO; DERWENT	OR	ON	2004/12/29 11:12
S77	134	S65 near S71	US-PGPUB; USPAT; EPO; DERWENT	OR	ON	2004/12/29 11:12
S78	0	S76 and S77	US-PGPUB; USPAT; EPO; DERWENT	OR	ON	2004/12/29 11:13
S79	832	S75 same S68	US-PGPUB; USPAT; EPO; DERWENT	OR	ON	2004/12/29 11:13
S80	547	S79 and S70	US-PGPUB; USPAT; EPO; DERWENT	OR	ON	2004/12/29 11:13
S81	202	S80 and S69	US-PGPUB; USPAT; EPO; DERWENT	OR	ON	2004/12/29 11:14
S82	3	S81 and S71	US-PGPUB; USPAT; EPO; DERWENT	OR	ON	2004/12/29 11:14
S83	579	Turn near packet	US-PGPUB; USPAT; EPO; DERWENT	OR	ON	2004/12/29 11:43
S84	186	Turn near protocol	US-PGPUB; USPAT; EPO; DERWENT	OR	ON	2004/12/29 11:44
S85	4	S83 and S84	US-PGPUB; USPAT; EPO; DERWENT	OR	ON	2004/12/29 12:00
S86	53	(709/245).ccls. and ("713").clas.	US-PGPUB; USPAT; EPO; DERWENT	OR	ON	2004/12/30 15:38
S87	4	S86 and (S75 or S69)	US-PGPUB; USPAT; EPO; DERWENT	OR	ON	2004/12/29 12:16
S88	3116	previous$ near packet	US-PGPUB; USPAT; EPO; DERWENT	OR	ON	2004/12/29 12:16
S89	2827	compar$ near packet	US-PGPUB; USPAT; EPO; DERWENT	OR	ON	2004/12/29 12:16

S90	41	S88 same S89	US-PGPUB; USPAT; EPO; DERWENT	OR	ON	2004/12/29 12:17
S97	1	((US "6496935" B1).pn. or (US "20040073704" A1).pn.) and rule$	US-PGPUB; USPAT	OR	ON	2004/12/30 16:09
S98	92882	(NAT) or (Network near address near translation)	US-PGPUB; USPAT; EPO; DERWENT	OR	ON	2004/12/30 14:31
S105	1	(US "20040260763" A1).pn. and overlap$	US-PGPUB; USPAT	OR	ON	2004/12/30 15:22
S106	53	(709/245).ccls. and ("713").clas.	US-PGPUB; USPAT; EPO; DERWENT	OR	ON	2004/12/30 15:38
S107	9	S106 and S98	US-PGPUB; USPAT; EPO; DERWENT	OR	ON	2004/12/30 15:40
S108	788	(multiple or many or (more near one)) with (NAT or NATs)	US-PGPUB; USPAT; EPO; DERWENT	OR	ON	2004/12/30 15:40
S110	45	S108 with (intranet or (private near network))	US-PGPUB; USPAT; EPO; DERWENT	OR	ON	2004/12/30 15:42
S111	42	S110 and (events or packet)	US-PGPUB; USPAT; EPO; DERWENT	OR	ON	2004/12/30 15:46
S112	6723	(map$ or rule) with overlap$	US-PGPUB; USPAT; EPO; DERWENT	OR	ON	2004/12/30 15:46
S113	42	S111 and S98	US-PGPUB; USPAT; EPO; DERWENT	OR	ON	2004/12/30 15:47
S114	987	S112 and S98	US-PGPUB; USPAT; EPO; DERWENT	OR	ON	2004/12/30 15:47
S115	3	S112 with S98	US-PGPUB; USPAT; EPO; DERWENT	OR	ON	2004/12/30 15:47

DataStar Web

Documents

Table of Contents

Collaborative intrusion detection system (CIDS): a framework for accurate and efficient IDS.

Accession number & update
8211914, C2005-01-6130S-211; 20041212.

Author(s)
Yu-Sung-Wu; Foo-B; Mei-Y; Bagchi-S.
Author affiliation
Sch of Electr & Comput Eng, Purdue Univ, West Lafayette, IN, USA.

Source
Proceedings. 19th Annual Computer Security Applications Conference, Las Vegas, NV, USA, 8-12 Dec. 2003.
Sponsors: Applied Comput. Security Associates.
In: p.234-44, 2003.
ISSN
ISBN: 0-7695-2041-3, CCCC: 1063-9527/03/ ($17.00).
Publication year
2003.
Language
EN.
Publication type
CPP Conference Paper.
Treatment codes
P Practical.

Abstract
We present the design and implementation of a ***collaborative intrusion detection*** system (CIDS) for accurate and efficient ***intrusion detection*** in a distributed system. CIDS employs multiple specialized ***detectors*** at the different layers - network, kernel and application - and a manager based framework for aggregating the alarms from the different ***detectors*** to provide a combined alarm for an ***intrusion.*** The premise is that a carefully designed and configured CIDS can increase the accuracy of ***detection*** compared to individual ***detectors,*** without a substantial degradation in performance. In order to validate the premise, we present the design and implementation of a CIDS which employs Snort, Libsafe, and a new kernel level IDS called Sysmon. The manager has a graph-based and a Bayesian network based aggregation method for combining the alarms to finally come up with a decision about the ***intrusion.*** The system is evaluated using a Web-based electronic store front application and under three different classes of attacks - buffer overflow, flooding and script-based attacks. The results show performance degradations compared to no ***detection*** of 3.9% and 6.3% under normal workload and a buffer overflow attack respectively. The experiments to evaluate the accuracy of the system show that the normal workload generates false alarms for Snort and the elementary ***detectors*** produce missed alarms. CIDS does not flag the false alarm and reduces the incidence of missed alarms to 1 of the 7 cases. CIDS can also be used to measure the propagation time of an ***intrusion*** which is useful in choosing an appropriate response strategy. (19 refs).

Descriptors
belief-networks; Internet; security-of-data.
Keywords
collaborative intrusion detection system; distributed system; specialized ***detectors;*** graph based aggregation method; Bayesian network based aggregation method; Web based electronic store; false alarms; missed alarms; ***event correlation;*** Bayesian network based ***detection.***
Classification codes
C6130S (Data security).
C6150N (Distributed systems software).
C1160 (Combinatorial mathematics).

The analysis of *event correlation* in *intrusion detection.*

USPTO Full Text Retrieval Options

Accession number & update
7901313, B2004-04-6210C-031, C2004-04-6130S-213; 20040301.

Author(s)
Chen-Xiaosu; Yin-Hongbin; Xiao-Daoju.

Author affiliation
Coll of Comput Sci & Tech, Huazhong Univ of Sci & Technol, China.

Source
Journal-of-Huazhong-University-of-Science-and-Technology (China), vol.31, no.4, p.30-3, April 2003. , Published: Editorial Board J. Huazhong Univ. of Sci. & Technol.

CODEN
HLDXE6.

ISSN
ISSN: 1671-4512.

Availability
SICI: 1671-4512(200304)31:4L.30:AECI; 1-T.

Publication year
2003.

Language
CH.

Publication type
J Journal Paper.

Treatment codes
P Practical.

Abstract
A method for the analysis of an ***event correlation*** is introduced based on the characteristics of the two kinds of relationships, that is, redundancy relationship and cause and effect relationship. Based on that, an architecture designed for ***event correlation*** analysis apparatus is presented. Practice shows that ***event correlation*** can decrease the number of alerts, reduce false alerts and discover high-level attack strategies effectively. (2 refs).

Descriptors
authorisation; computer-network-management.

Keywords
event correlation; intrusion detection; redundancy relationship; cause and effect relationship; false alert reduction; high level attack strategies.

Classification codes

B6210C	(Network management).
B6210L	(Computer communications).
C6130S	(Data security).
C5620	(Computer networks and techniques).

A *cyber-event correlation* framework and metrics.

USPTO Full Text Retrieval Options

Accession number & update
7771811, C2003-12-6130S-032; 20031101.

Author(s)
Kang-M-H; Mayfield-T.

Author affiliation
Mitretek Systems, Falls Church, VA, USA.

Source
System Diagnosis and Prognosis: Security and Condition Monitoring Issues III, Orlando, FL, USA, 21 April 2003.
Sponsors: SPIE.
In: Proceedings-of-the-SPIE-The-International-Society-for-Optical-Engineering (USA), vol.5107, p.72-82, 2003.

CODEN
PSISDG.

ISSN
ISSN: 0277-786X, CCCC: 0277-786X/03/ ($15.00).

Availability
SICI: 0277-786X(2003)5107L.72:CECF; 1-A.

Publication year
2003.

Language
EN.

Publication type
CPP Conference Paper, J Journal Paper.

Treatment codes
P Practical.

Abstract
In this paper, we propose a ***cyber-event*** fusion, ***correlation,*** and situation assessment framework that, when instantiated, will allow cyber defenders to better understand the local, regional, and global cyber-situation. This framework, with associated metrics, can be used to guide assessment of our existing cyber-defense capabilities, and to help evaluate the state of ***cyber-event correlation*** research and where we must focus our future ***cyber-event correlation*** research. The framework, based on the ***cyber-event*** gathering activities and analysis functions, consists of five operational steps, each of which provides a richer set of contextual information to support greater situational understanding. The first three steps are categorically depicted as increasingly richer and broader-scoped contexts achieved through ***correlation*** activity, while in the final two steps, these richer contexts are achieved through analytical activities (situation assessment, and threat analysis & prediction). Category 1 ***Correlation*** focuses on the ***detection*** of suspicious activities and the ***correlation*** of events from a single ***cyber-event*** source. Category 2 ***Correlation*** clusters the same or similar events from multiple ***detectors*** that are located at close proximity and prioritizes them. Finally, the events from different time periods and ***event*** sources at different location /regions are ***correlated*** at Category 3 to recognize the relationship among different events. This is the category that focuses on the ***detection*** of large-scale and coordinated attacks. The situation assessment step (Category 4) focuses on the assessment of cyber asset damage and the analysis of the impact on missions. The threat analysis and prediction step (Category 5) analyzes attacks based on attack traces and predicts the next steps. Metrics that can distinguish ***correlation*** and cyber-situation assessment tools for each category are also proposed. (4 refs).

Descriptors
open-systems; security-of-data; sensor-fusion.

Keywords
cyber ***event*** fusion; situation assessment framework; cyber defenders; cyber defense capabilities; contextual information; suspicious activities; attack traces; ***intrusion detection;*** data fusion.

Classification codes

C6130S (Data security).
C5260A (Sensor fusion).
C6150N (Distributed systems software).

Digital object identifier

http://dx.doi.org/10.1117/12.488029.

The importance of *event correlation* for effective security management.

Accession number & update

7550582, C2003-04-0310-011; 20030317.

Author(s)

Caldwell-M.

Source

Information-Systems-Control-Journal (USA), vol.6, p.36-8, 2002. , Published: Inf. Syst. Audit. & Control Assoc.

CODEN

ISYJFS.

ISSN

ISSN: 1526-7407, CCCC: 1526-7407/02/ ($2.50+0.25).

Availability

SICI: 1526-7407(2002)6L.36:IECE; 1-J.

Publication year

2002.

Language

EN.

Publication type

J Journal Paper.

Treatment codes

G General or Review.

Abstract

Security teams try to ***detect*** attacks and internal misuse by wading through and making sense of an overwhelming amount of raw ***event*** data generated from firewalls, ***intrusion detection*** systems, vulnerability reports, routers, computer systems and other devices. This process does not provide the coherent view of their networks necessary to successfully manage threats. A solution for this problem is an emerging security category called security ***event*** management (SEM). SEM systems automatically aggregate and ***correlate*** security ***event*** log data across multiple types of security devices allowing security analysts to focus on critical tasks that require human intelligence, such as investigating the source of attacks and responding to them. There are a wide variety of SEM solutions, but at the core of all of these solutions is the ability to ***correlate*** alerts across a heterogeneous security environment. ***Correlation*** of ***event*** data is critical to uncover security breaches because security incidents are made up of a series of events that occur at various touch points throughout a network. Unlike network management, which typically is exception-based or a one-to-one process, security management is far more complex. An attack typically touches a network at multiple points and leaves marks or breadcrumbs at each. By finding and following that breadcrumb trail, a security analyst can ***detect*** and hopefully prevent the attack.

Descriptors

business-data-processing; DP-management; information-systems; security-of-data.

Keywords

event correlation; enterprise information security; security ***event*** management; security ***event*** log data; heterogeneous security environment; alerts.

Classification codes

C0310 (EDP management).
C6130S (Data security).
C7100 (Business and administration).

Decentralized *event correlation* for *intrusion detection.*

Accession number & update

7301503, C2002-07-6130S-101; 20020617.

Author(s)

Krugel-C; Toth-T; Kerer-C; Ed. by Kim-K.

Author affiliation

Distributed Syst ***Group,*** Technische Univ Wien, Vienna, Austria.

Source

Information Security and Cryptology - ICISC 2001. 4th International Conference. Proceedings, Seoul, South Korea, 6-7 Dec. 2001.
Sponsors: Korea Inst. Inf. Security & Cryptology (KIISC).
In: p.114-31, 2002.

ISSN

ISBN: 3-540-43319-8.

Publication year

2002.

Language

EN.

Publication type

CPP Conference Paper.

Treatment codes

A Application; P Practical.

Abstract

Evidence of attacks against a network and its resources is often scattered over several hosts. ***Intrusion detection*** systems (IDS) which attempt to ***detect*** such attacks therefore have to collect and ***correlate*** information from different sources. We propose a completely decentralized approach to solve the task of ***event correlation*** and information fusing of data gathered from multiple points within the network. Our system models an ***intrusion*** as a pattern of events that can occur at different hosts and consists of collaborating sensors deployed at various locations throughout the protected network installation. We present a specification language to define ***intrusions*** as distributed patterns and a mechanism to specify their simple building blocks. The peer-to-peer algorithm to ***detect*** these patterns and its prototype implementation, called Quicksand, are described. Problems and their solutions involved in the management of such a system are discussed. (16 refs).

Descriptors

safety-systems; security-of-data.

Keywords

decentralized ***event correlation; intrusion detection; intrusion detection*** systems; information fusing; collaborating sensors; specification language; peer to peer algorithm; Quicksand.

Classification codes

C6130S (Data security).

Information Security and Cryptology - ICISC 2001. 4th International Conference. Proceedings (Lecture Notes in Computer Science Vol.2288).

Accession number & update

7301493, B2002-07-0100-073, C2002-07-6130S-091; 20020617.

Author(s)

Ed. by Kim-K.

Source

Information Security and Cryptology - ICISC 2001. 4th International Conference. Proceedings (Lecture Notes in Computer Science Vol.2288), Seoul, South Korea, 6-7 Dec. 2001.
Sponsors: Korea Inst. Inf. Security & Cryptology (KIISC).
Published: Springer-Verlag, Berlin, Germany, xiii+456 pp, 2002.

ISSN

ISBN: 3-540-43319-8.

Publication year

2002.

Language

EN.

Publication type

CPR Conference Proceedings.

Abstract

The following topics are dealt with: practical security in public-key cryptography; truncated differential cryptanalysis of Camellia; cryptanalysis of nonlinear filter generators with {0,1}-metric Viterbi decoding; design and analysis of fast provably secure public-key cryptosystems based on a modular squaring; decentralized ***event correlation*** for ***intrusion detection;*** enhancing the security of cookies; binary codes for collusion-secure fingerprinting; off-line authentication using watermarks; constructions of cheating immune secret sharing; an optimistic multi-party fair exchange protocol with reduced trust requirements; content extraction signatures; an efficient and provably secure threshold blind signature; a distributed light-weight authentication model for ad-hoc networks; secure authorisation agent for cross-domain access control; in a mobile computing environment; protecting general flexible itineraries of mobile agents; RSA speedup with residue number system immune against hardware fault cryptanalysis; a fast scalar multiplication method with randomized projective coordinates on a Montgomery-form elliptic curve secure against side channel attacks.

Descriptors

cryptography.

Keywords

public key cryptography; truncated differential cryptanalysis; nonlinear filter generators; Viterbi decoding; provably secure public key cryptosystems; modular squaring; decentralized ***event correlation;*** collusion secure fingerprinting; authentication; fair exchange protocol; content extraction signatures; RSA speedup; hardware fault cryptanalysis; Montgomery form elliptic curve; security.

Classification codes

B0100 (General electrical engineering topics).
B6120D (Cryptography).
C6130S (Data security).
C1260C (Cryptography theory).

Copyright statement

Event correlation.

Accession number & update

6926943, C2001-06-5620W-056; 20010521.

Author(s)
Yongseok–Park.
Author affiliation
Coree Networks, NJ, USA.
Source
IEEE–Potentials (USA), vol.20, no.2, p.34–5, April–May 2001. , Published: IEEE.
CODEN
IEPTDF.
ISSN
ISSN: 0278–6648, CCCC: 0278–6648/2001/ ($10.00).
Availability
SICI: 0278–6648(200104/05)20:2L.34:EC; 1–2.
Publication year
2001.
Language
EN.
Publication type
J Journal Paper.
Treatment codes
P Practical.
Abstract
The advent of modern computer technology has enabled the development of many complex man–made systems. These include discrete manufacturing systems, communication networks, computer systems, traffic control systems, and inventory systems. A ***common*** characteristic of these systems is that they have discrete states (e.g., idle, processing, queue empty/full, and normal/faulty). Also, their state transition is triggered by events (e.g., part arrival/dispatch, alarms, commands, and timeout). For this reason, these systems are called discrete ***event*** systems or ***event–driven*** systems. As today's industry moves towards more complex, distributed and heterogeneous discrete ***event*** systems, there is a growing need for integration, consolidation, ***correlation,*** and distribution of the events coming from the systems. ***Event correlation*** achieves those objectives using methods borrowed mostly from artificial intelligence and formal methods. Historically, ***event correlation*** systems were developed for real–time monitoring of many classical mission–critical systems such as power plant and water/gas /oil distribution systems. Recently, it has been spreading into new areas such as messaging, network management and computer ***intrusion detection.*** (4 refs).
Descriptors
discrete–event–systems; Internet.
Keywords
event correlation; discrete states; state transition; discrete ***event*** systems; ***event*** driven systems; formal methods; artificial intelligence.
Classification codes
C5620W (Other computer networks).
C6150N (Distributed systems software).

Search strategy

No.	Database	Search term	Info added since	Results
1	INZZ	intrus$ NEAR detect$	unrestricted	2028
2	INZZ	(collaborative OR common OR related OR correlat$ OR group$4) NEAR event	unrestricted	2943
6	INZZ	1 AND 2	unrestricted	16

Saved: 28-Dec-2004, 17:12:54 CET

DataStar Web

Documents

Table of Contents

Enlisting *event* patterns for cyber battlefield awareness.

Accession number & update
6498877, C2000-03-6150N-113; 20000201.

Author(s)
Perrochon-L; Eunhei-Jang; Kasriel-S; Luckham-D-C.
Author affiliation
Stanford Univ, CA, USA.

Source
Proceedings DARPA Information Survivability Conference and Exposition. DISCEX'00, vol.2, Hilton Head, SC, USA, 25-27 Jan. 2000.
Sponsors: DARPA.
In: p.411-22 vol.2, 1999.
ISSN
ISBN: 0-7695-0490-6, CCCC: 0 7695 0490 6/99/ ($10.00).
Publication year
1999.
Language
EN.
Publication type
CPP Conference Paper.
Treatment codes
P Practical.

Abstract
Cyber warfare consists to a large degree of reaction to activities happening in the information infrastructure. Better knowledge of the status of this infrastructure at any time allows more appropriate reactions. Context-based ***event correlation*** can provide a more appropriate view of the cyber battlefield by providing users a view on the desired level of abstraction. We informally introduce context as the temporal and causal relations between events. ***Event correlation*** based on ***event*** patterns in a declarative language means we specify what to ***detect,*** instead of how to ***detect.*** We describe the Stanford University context-based ***event correlator*** that is able to process events on-line, as they are generated. It can be reconfigured dynamically while it is running. On the example of ***intrusion detection,*** we show how Complex ***Event*** Processing (CEP) increases ***detection*** rate, reduce false alarms, and ***detect*** large-scale attack patterns at an early stage. (33 refs).

Descriptors
computer-network-management; security-of-data; supervisory-programs.
Keywords
event patterns; cyber battlefield awareness; cyber warfare; information infrastructure; context based ***event correlation;*** declarative language; Stanford University context based ***event correlator; intrusion detection;*** large scale attack patterns.
Classification codes
C6150N (Distributed systems software).
C6130S (Data security).

Search strategy

No.	Database	Search term	Info added since	Results
1	INZZ	intrus$ NEAR detect$	unrestricted	2028
2	INZZ	(collaborative OR common OR related OR correlat$ OR group$4) NEAR event	unrestricted	2943
3	INZZ	NAT OR Network NEAR address NEAR translation	unrestricted	376487
4	INZZ	1 AND 2 AND 3	unrestricted	1
5	INZZ	2 AND 3	unrestricted	135
6	INZZ	1 AND 2	unrestricted	16

Saved: 28-Dec-2004, 17:11:55 CET